Behavioral Analytics

How to Protect IP, Detect Compromised Accounts, and Reduce Insider Risk
The brave new world of Data and Security Analytics

For every action, file, applications, and user within a network, data is continually created. The concept of using analytics to identify and subsequently thwart potential threats is a logical next step in the evolutionary journey of cybersecurity.

This is where Behavioral Analytics comes into play—delivering visibility into employee activities, behaviors, and relationships by integrating unstructured, context-rich data streams with structured data.

More so, analytic models enable entities and events to be scored and prioritized through multiple lenses across all data streams—previously unavailable to security teams. This same technology also integrates with Active Directory, SIEM, EDRs, and key data sources to offer true situational awareness and a powerful forensic lens that radically enhances internal investigations.
Traditional, black-box UBA tools are often limited to structured data sources, analyzed in disparate systems, with a fixed analytics configuration. In contrast, more modern solutions deliver powerful analytic capabilities that allow security teams to address evolving security use cases and perform real-time ad-hoc analysis, including advanced search across all data sets. Better yet, modern analytics can be tuned without additional programming, enabling a more nimble response to security threats.

Behavioral Analytics solutions are fundamentally built to scale—storing structured and unstructured data and scaling horizontally to grow with the business. They should also provide variable levels of access and administrative controls so that users can rely on the technology to work in any deployment.
Behavioral Analytics enables rapid review of non-compliant activity through various user interfaces—enabling analysts and managers to investigate quickly, review, escalate, and take action. This also leads to the management of what is referred to as data entitlements—data required by both internal controls and externally driven data privacy concerns.

Behavioral Analytics systematically identifies behavior changes that may indicate current or potentially illegal, unwanted or non-compliant activity by employees using sentiment and content analysis. This is achieved through intelligent prioritization techniques that flag events of interest and alerts based on the analysis of content and metadata patterns.
Behavioral Analytics also significantly reduces false positives through smart, practical NLP applications, complex lexicons for any language, and text identification technology that recognizes disclaimers and quoted text from threaded emails.

Visualizations can be specifically developed to unlock an analyst's inference capabilities and deliver full context around relevant activities. This enables them to understand who, what, and when quickly, and the how of employee actions. Simultaneously, content classifications can also be created to identify and filter out non-relevant communications like bulk mail, third-party mailers, and more.
Behavioral Analytics solutions can now deliver advanced data science models without heavy professional services commitment. Deployment has become highly flexible, with solutions ranging from on-prem, virtual private cloud, and even appliance-based options.

Contact us for a free consultation or to receive a free Cloud Security Audit to assess the effectiveness of your current cyber security initiatives.